العنوان:	سياسة المشروع الإماراتي لمواجهة الجرائم الإلكترونية
المصدر:	مجلة الفكر الشرطي - مركز بحوث الشرطة - القيادة العامة لشرطة الشارقة - الإمارات
المؤلف الرئيسي:	حسن، عبيد صالح
المجلد/العدد:	مج24, ع95
محكمة:	نعم
التاريخ الميلادي:	2015
الشهر:	أكتوبر
الصفحات:	21 - 52
رقم MD:	683729
نوع المحتوى:	بحوث ومقالات
قواعد المعلومات:	HumanIndex
مواضيع:	الجرائم الإلكترونية، السياسة الجنائية، الاجراءات الجزائية، العقوبات، الإمارات
رابط:	http://search.mandumah.com/Record/683729

سياسة المشرع الإماراتي لمواجهة الجرائم الإلكترونية[1]

DOI: 10.12816/0014752

العقيد الدكتور. عبيد صالح حسن [2]

مدير إدارة مركز بحوث شرطة الشارقة – الإمارات

مستخلص

تتناول هذه الدراسة سياسة المشرع الإماراتي تجاه الخطر الدائم للجرائم الإلكترونية التي تزداد مهدداتها يوما بعد يوم وذلك من خلال استعراض ماهية الجرائم الإلكترونية وأنماطها وخصائصها وسماتها ومخاطرها والتعرف بالتشريعات الموجودة بدولة الإمارات للتعامل مع تلك النوعية من الجرائم، وأخيراً موقف المشرع الإماراتي. وقد تمثلت مشكلة الدراسة في أنماط متعدد للجرائم الإلكترونية التي تطلبت مواجهة مستمرة ومراجعة دائمة للسياسة التشريعية الإماراتية بشأن تلك الجرائم، وتسعى هذه الدراسة إلى التعرف على واقع الجريمة الإلكترونية في الإمارات والوقوف على التشريعات الصادرة بشأنها والتعرف على التوجهات الفكرية لدى المشرع الإماراتي في ظل المتغيرات المتسارعة في عصر الثورة التقنية وقد اعتمدت الدراسة منهج الوصف التحليلي من خلال التعرض لماهية الجرائم الإلكترونية ومفهومها وأنماطها وخصائصها وسماتها ومخاطرها وموقف المشرع الإماراتي وسياسته في القانون الصادر عام 2012 م. ولقد انتهت الدراسة إلى مجموعة النتائج أبرزها وجود مخاطر وأضرار تشكلها الجرائم الإلكترونية بأنواعها المختلفة وعدم اقتصارها على جانب، وإنما هي مخاطر متعددة ومتنوعة وأن هناك جوانب قانونية جديدة يجب على المشرع القانوني في الإمارات مراعاتها عند إعداد وصياغة القوانين المنظمة للتعامل مع الجرائم الإلكترونية بأنواعها المختلفة. وقد انتهت الدراسة إلى مجموعة من التوصيات تمثلت فيما يلي: ضرورة التعاون والتنسيق الدولي مع المنظمات والمؤسسات التشريعية للتعرف على الاتجاهات التشريعية المختلفة المتبعة في تلك البلدان للاستفادة منها في دولة الإمارات، والمراجعة المستمرة والدورية من قبل المشرع الإماراتي للسياسة التشريعية الموضوعة للتعامل مع الجرائم الإلكترونية مع العمل على تعديلها في حال بيان عدم فاعليتها والحرص في السياسات التشريعية المتبعة على مراعاة مدى التناسب أو التوازن بين جسامة الضرر أو الخطر ومقدار العقوبة.

مفردات البحث:

المشرع الإماراتي – السياسات الجنائية – الجرائم الإلكترونية – الثورة التكنولوجية والتقنية– الإجراءات الجزائية – العقوبات.

1- ورد هذا البحث للدورية بتاريخ أغسطس 2015 م، وقيد تحت رقم 2015/89 جديد، وأحيل للتحكيم في سبتمبر 2015 م، وأجيز للنشر في أكتوبر 2015 م.

2- حصل العقيد الدكتور عبيد صالح حسن على درجة الدكتوراه في علوم الشرطة من أكاديمية الشرطة المصرية وهو يعمل مديراً لإدارة مركز بحوث شرطة الشارقة بالإضافة إلى عضويته في اللجنة العليا في برنامج الشارقة للوقاية من الجريمة واللجنة التنسيقية لمراكز البحوث بوزارة الداخلية، وقد حصل على العديد من الأوسمة منها: وسام وزير الداخلية من الطبقة الأولى، وجائزة الشارقة للتفوق العلمي ووسام رئيس الدولة للتميز، وجائزة راشد للتميز العلمي. وله العديد من البحوث والكتب المنشورة كما أنه محاضر معتمد في مجالات إدارة الشرطة وتقنية المعلومات وإدارة المكاتب والسكرتارية والجرائم الإلكترونية والإبداع والابتكار الإداري.

Policies of UAE Legislator in E - Crime Confrontation [(1)]

DOI: 10.12816/0014752

Colonel Dr. Obeid Saleh Hassan [(2)]

Director of Sharjah Police Research Center – UAE

Abstract:

Study deals with this subject by defining E. Crime and enumerating its types, features, characteristics and risks and also throwing spotlight on UAE legislations dealing with such type of crimes. Study also sets forth attitude of UAE legislator from such crimes. Study handles this subject owing to the relentless danger of E- crimes and their ever increasing risks. Study argues that confrontation of such crimes and review of associated legislations should be continuous. Study endeavors to identify the volume of E- Crimes in UAE; examine associated legislations and identify attitudes of UAE legislator. Study used descriptive analytical approach in defining E-Crimes, enumerating its types, features, characteristics, risks and attitude of UAE legislator in the law issued in 2012. Study summed up with a host of findings, the most important of which is that E. Crimes' risks are not limited to one aspect, but rather extends to many, and that there are new legal aspects for UAE legislator to reconsider in the drafting of laws dealing with the various types of E. Crimes. Study also summed up with numerous recommendations including, the need for cooperation and coordination with international legislative bodies with a view to identifying the various legislative aspects adopted in various countries in order to benefit from them in UAE. Recommendations also included the importance of UAE Legislations conducting a continuous review for the existing legislative policies dealing with E. Crimes; trying to amend them in case they prove ineffective and taking into account proportionality of punishment to the harm caused by the crime.

Keywords:

UAE Legislator – Criminal Policies – E. Crimes – Technical and Technological Revolution – Penal Procedures – Penalties.

1-**Manuscript:** was submitted in August 2015 under No (89/2015, New), refereed in 2015 and approved for publication in October 2015.

2-**Biography:** Colonel Dr. Obeid Salih Hassan Ali attained his doctoral degree in Police Sciences from Police Academy – Egypt. He is currently the director of Sharjah Police Research Center. He is also member of Higher Committee of Sharjah Crime Prevention Program and the Coordinative Committee of Research Centers at Ministry of Interior. He has been awarded numerous decorations, including Minister of Interior's Decoration (first class), and UAE's president Decoration for Excellence. He has been also awarded Sharjah Award for Scientific Distinction and Rashid Award for Scientific Excellence. He published a host of researches and books. He is also an accredited lecturer in fields of police management, IT, Secretariat, Offices Management, E. Crime and Administrative Innovation.

مقدمة:

أدّت الثورة التكنولوجية التي شهدها العالم خلال العقود الأخيرة من القرن العشـــرين إلى ظهور أنماط إجرامية جديدة لم تكن مألوفة من قبل. وهي ما أطلـــق عليهـــا "الجـــرائم الإلكترونية" والتي تعتمد في ارتكابها على استخدام أجهزة الحاســـوب وشـــبكة الإنترنـــت والبرامج التقنية المختلفة.

وقد أدّى التطور المتسارع في النظم التقنية والبرامج والشبكات الإلكترونية المرتبطة بها – في ضوء ما وفرته من سبل عدة للاتصال والتواصل ونقـــل البيانـــات والمعلومـــات وتخزينها والاستفادة منها كذلك في تلبية الاحتياجات الرئيسية لتطوير وتحسين بيئة العمل– إلى زيادة اعتماد المؤسسات سواء الحكومية أم الخاصة على تلك الأنظمة بأدواتها المختلفة.

وقد حفزت المزايا والإيجابيات العديدة التي اتسمت بهـــا وحققتهـــا تلـــك الطفـــرة الإلكترونية الدول والأفراد على حد سواء على اقتنائها واستخدامها كأداة رئيسية في مجالات عدة سواء على المستوى الشخصي أم المؤسسي لا سيما دولة الإمارات العربية المتحدة في ضوء ما تتمتع به من إمكانات مادية متميزة مكّنتها من توفير كافة النظم والأدوات والبرامج الإلكترونية الأكثر تقدماً، وأيضاً في ضوء سعيها الدائم لاستخدام أفضل النظم التي تمكنهـــا من التطوير والتحسين المستمر حتى أصبحت كل مؤسساتها تعتمد بصـــورة كليـــة علـــى التقنيات في مجالات الحياة المختلفة.

ولا شك أن هذا الأمر قد أوجد تحديًّا وهاجساً ليس على المستوى الأمني فقط بل على كافة المستويات في ضوء ما تم ارتكابه من جرائم إلكترونية على المستوى العالمي اعتمـــدت في ارتكابها على التقنيات الإلكترونية المستخدمة والتي شكلت مخاطر ومهددات عدة لم تقتصر على جانب واحد فقط، لا سيما في ضوء ما أصبحت تمثله الأنظمـــة والأدوات الإلكترونيـــة المختلفة من عصب رئيسي ومحرك فاعل للكثير من متطلبات الحيـــاة وأنظمتهـــا بـــالمجتمع الخليجي، كما يمكن القول بأنها أصبحت تمثل مستودع السر للحفاظ على الكثير من الثـــروات والمقتنيات، وأيضاً في ضوء ما كشفت عنه الكثير من الجرائم الإلكترونية المرتكبـــة مـــن أن

أضرارها فاقت بكثير ما أدّت إليه الجرائم التقليدية الأخرى من أضرار وأخطار للعديد من العوامل والأسباب والتي من بينها سهولة ارتكابها وتوافر المعرفة والمهارة التقنية لدى مرتكبيها وحرصهم الدائم على تطوير قدراتهم مما يمكنهم من ارتكاب المزيد من تلك الجرائم، وأيضاً لما تحققه من فوائد مادية أو معنوية عدة لمرتكبيها، وأيضا لاختلافها عن الجرائم التقليدية التي تتسم بمحدودية المكان والزمان لكونها في البعض منها تعدّ من الجرائم العابرة للوطنية والتي تستلزم للوقاية منها ومكافحتها تعاوناً دوليًّا وإقليميًّا قد يصعب في الكثير من الأحيان تحقيقه، وكذلك الحاجة إلى قواعد ونظم تعدّ أكثر تعقيداً من تلك اللازمة للتعامل مع الجرائم التقليدية، إضافة إلى ضرورة توافر مهارات وقدرات خاصة برجال الأمن تختلف كثيراً عن تلك اللازمة للتعامل مع الجرائم الأخرى.

وفي ضوء ذلك، قامت الدولة في ضوء ما اكتشفته من الخطر الداهم للجرائم الإلكترونية وتزايد مهدداتها يوماً بعد يوم بإصدار التشريعات لغرض الوقاية والمكافحة لتلك الجرائم، ومن أمثلة ذلك القانون الاتحادي الإماراتي رقم (2) لسنة 2006 م في شأن مكافحة جرائم تقنية المعلومات، إلا أنه بالرغم من العمل بتلك التشريعات فإن الجرائم الإلكترونية ما زالت تشكل خطراً يتطلب المزيد من البحث والدراسة لغرض الوقوف على أفضل السبل لمكافحتها والوقاية من مخاطرها سواء القديمة أم المستجدة التي أوجدتها شبكات التواصل الاجتماعي.

وفي هذا السياق يجب أن نشير إلى ما قاله أستاذ القانون الجنائي الفرنسي الشهير "جورج لبفاستر" إنّ هناك ما يسمى "بوطنية " السياسة التشريعية، بمعنى أن لكل دولة سياسة تشريعية تتبعها، وبالتالي لا يتصور أن تتطابق سياستان تشريعيتان لدولتين أو أكثر تطابقاً تامًّا في ضوء المتغيرات الاجتماعية والاقتصادية والأمنية والسياسية لكل منها.

من أجل ذلك سوف تعنى تلك الدراسة ببيان سياسة المشرع الإماراتي لمواجهة الجرائم الإلكترونية، من خلال البيان لماهية الجرائم الإلكترونية وأنماطها وخصائصها وسماتها ومخاطرها، وكذلك التعريف بالتشريعات الموجودة بدولة الإمارات للتعامل مع تلك

النوعية من الجرائم، وأخيراً بيان موقف المشرع الإماراتي وسياسته في التعامل مع تلك النوعية من الجرائم.

مشكلة الدراسة:

تتمثل مشكلة الدراسة فيما تشكله الجرائم الإلكترونية بأنماطها المختلفة من مخاطر عدة على المجتمع، لا سيما في ظل التطور الهائل في الأدوات والوسائل الإلكترونية المستخدمة، وبما يهدد ما تم تحقيقه من طفرة تنموية. وكذلك تهديدها المستمر للثروات والبنية الإلكترونية التي أصبحت عمداً رئيسيًّا لتسيير كافة الأنشطة الاقتصادية والإدارية والمالية وغيرها ولحفظ كافة الوثائق ولتحقيق التغذية المعلوماتية اللازمة لغرض حل المشكلات والقضايا بصورة فاعلة.

وإضافة إلى ما سبق، فإنّ تلك الجرائم تعدّ أكثر خطورة على أمن المجتمع لكون البعض من أنماطها من الجرائم العابرة للوطنية والتي يتطلب الأمر لملاحقة مرتكبيها نمطاً قانونيًّا وإجرائيًّا يختلف عن المتبع في التعامل مع الجرائم التقليدية الأخرى. كما تتزايد خطورة الجرائم الإلكترونية لوجود العديد من أنماطها. وأيضا للتطور المستمر في التقنيات الإلكترونية والتي أوجدت مجالاً واسعاً لإساءة استغلالها من قبل البعض من الدول والجماعات لارتكاب الأفعال والسلوكيات التي من شأنها تهديد الأمن القومي والوحدة الوطنية وتعريض النسيج الاجتماعي للتمزق وإحداث الفوضى والتخريب بمؤسسات المجتمع وبنيته سواء السياسية أم الاقتصادية أم الاجتماعية.

وبالرغم ممّا وضعه المشرع الإماراتي من تشريعات للتصدي للجرائم الإلكترونية إلا أن زيادة فاعلية مواجهة تلك الجرائم يتطلب مراجعة السياسة التشريعية للمشرع الإماراتي للتعرف على مدى مواكبتها لتلك النوعية من الجرائم ومدى الحاجة إلى مراجعتها لتتواءم مع مخاطر تلك الجرائم.

أهمية الدراسة:

تتمثل أهمية تلك الدراسة في الآتي:

1. استجلاء موقف المشرع الإماراتي حيال الجرائم الإلكترونية تلك النوعية من الجرائم المستجدة والتي تعد نتاج الثورة التكنولوجية والتقنية وتمثل أخطر إفرازاتها السلبية على المجتمع في نواحٍ عدة.
2. يسهم البحث في مجال التعرف على السياسة التشريعية في إثارة العديد من الجوانب التي ستساعد المشرع في التعرف على النواحي الواجب تطويرها وتحديثها في التشريعات.
3. إيضاح المخاطر والمهددات التي تشكلها الجريمة الإلكترونية بالمجتمع سيكون من شأنه تكاتف الجهود والتوجه نحو إيجاد سياسات تشريعية أكثر فاعلية في الحد أو المنع لتلك الجرائم.
4. بيان الأدوات التشريعية المستخدمة من قبل المشرع الإماراتي لغرض تفعيل سياسته التشريعية سواء فيما يتعلق بقواعد الإجراءات الجزائية أم النصوص العقابية ومدى ملاءمة كل منها في التصدي والتعامل مع الجرائم الإلكترونية.
5. إيضاح الأفعال والسلوكيات التي تعدّ أو تشكّل من وجهة نظر المشرع الإماراتي جريمة إلكترونية، ومن ثمّ بيان موقف المشرع الإماراتي حيالها.

أهداف الدراسة:

تسعى تلك الدراسة إلى تحقيق الأهداف التالية:

1. التعريف بواقع الجرائم الإلكترونية وأنماطها المرتكبة، ومن ثم التعرف على مخاطرها والآثار التي نجمت عنها.
2. الوقوف على التشريعات الصادرة بدولة الإمارات العربية المتحدة لمواجهة الجرائم الإلكترونية ومعاقبة مرتكبيها.
3. التعرف على التوجهات الفكرية لدى المشرع الإماراتي عند قيامه بصياغة التشريعات المتعلقة بمواجهة الجرائم الإلكترونية ومعاقبة مرتكبيها وهو ما يطلق عليه السياسة التشريعية.

4. إبراز اهتمام المشرع الإماراتي ومدى مواكبته للمتغيرات المتسارعة لعصر الثورة التقنية وإفرازاته للحفاظ على أمن المجتمع من كافة مخاطرها ومهدداتها.

تساؤلات الدراسة:

تسعى تلك الدراسة إلى الإجابة على التساؤلات التالية:

1. ماهية الجرائم الإلكترونية؟
2. ما هي أنماط الجرائم الإلكترونية؟
3. ما هي خصائص وسمات الجرائم الإلكترونية؟
4. ما هي مخاطر الجرائم الإلكترونية؟
5. ما هي التشريعات الموجودة بدولة الإمارات للتعامل مع تلك النوعية من الجرائم؟
6. ما هو موقف المشرع الإماراتي وسياسته في التعامل مع تلك النوعية من الجرائم؟

منهجية الدراسة:

سوف يتم الاعتماد عند إجراء تلك الدراسة على المنهج الوصفي التحليلي وذلك من خلال الوصف والبيان لماهية الجرائم الإلكترونية وأنماطها وخصائصها وسماتها ومخاطرها، وكذلك التعريف بالتشريعات الموجودة بدولة الإمارات للتعامل مع تلك النوعية من الجرائم، وأخيراً بيان موقف المشرع الإماراتي وسياسته في التعامل مع تلك النوعية من الجرائم.

تقسيمات الدراسة:

سوف يتم تقسيم الدراسة على النحو التالي: **المبحث الأول:** ماهية الجرائم الإلكترونية حيث يتناول **المطلب الأول:** مفهوم الجرائم الإلكترونية، **والمطلب الثاني:** أنماط الجرائم الإلكترونية. **والمبحث الثاني:** خصائص وسمات الجرائم الإلكترونية ومخاطرها حيث يتناول **المطلب الأول:** خصائص وسمات الجرائم الإلكترونية، **والمطلب الثاني:** مخاطر الجرائم الإلكترونية. **والمبحث الثالث:** موقف وسياسة المشرع الإماراتي اتجاه الجرائم

الإلكترونية حيث يتناول المطلب الأول: التشريع الإمـــاراتي الخـــاص بمواجهـــة الجـــرائم الإلكترونية، والمطلب الثاني: التعديلات التي أجراها المشرع الإماراتي علـــى التشـــريعات المتعلقة بالجرائم الإلكترونية، والمطلب الثالث: اتجاه وسياسة المشـــرع الإمـــاراتي تجـــاه الجرائم الإلكترونية بالقانون الجديد الصادر عام 2012 م. ثم الخاتمة والنتائج والتوصيات.

المبحث الأول
ماهية الجرائم الإلكترونية

شهد العالم خلال العقود الأربع الأخيرة تطوراً علميًّا متسارعاً كان من أبرز ملامحه ما أطلق عليه "الثورة التكنولوجية" والتي أدّت إلى الغزو التقني لكافة مجالات الحياة حيـــث أصبحت الأدوات والوسائل الإلكترونية أمراً لا غنى عنه في المؤسسات الحكومية والخاصة وكذلك لدى الأفراد بالمجتمع، كما أصبح لدى الغالبية العظمى من الجمهور المهارة والقدرة على استخدام تلك الأدوات والتعامل معها بكفاءة عالية.

ولا ينكر أحد أن تلك الثورة التكنولوجية كان لها العديـــد مـــن الفوائـــد والنـــواحي الإيجابية في كثير من نواحي الحياة، إلا أنه على الجانب الآخر كانت لها أيضاً البعض من الإفرازات السلبية نتيجة الميول الإجرامية لدى البعض في إساءة استخدام الأدوات والبرامج الإلكترونية واستغلال إمكانيات "الشبكة العنكبوتية" في سهولة التواصل ونقل المحتويات ممّا أدّى إلى ظهور نوعية جديدة من الجرائم وهي "الجرائم الإلكترونية".

وقد تعددت وتنوعت أنماط الجرائم الإلكترونية وأهداف ارتكابها وهو الأمر الـــذي زاد من خطورتها على أمن المجتمعات والمؤسسات والأفراد سواء على المستوى الدولي أم الإقليمي أم المحلي، ومن أمثلة تلك الجرائم النصب والاحتيال الإلكتروني، السرقة للأمـــوال وللمعلومات باستخدام البرامج الإلكترونية، الاختراق والتدمير للبرامج، ونشر الفيروســـات، الابتزاز والاستغلال الجنسي.

وتتمثل خطورة الجرائم الإلكترونية في أن مرتكبيها يمتلكون أدوات المعرفة التقنية والفنية ولديهم المهارات ووسائل الإقناع وإضفاء المصداقية على أفعالهم مما يؤدي إلى اندفاع الضحايا إلى الوقوع في براثنهم. كما تتضح خطورة تلك الجرائم في كونها تمس بالكيانات المؤسسية والاقتصادية والمالية وبالحياة الخاصة للأفراد كما تلحق بالأعمال التجارية الخسائر الفادحة وتنال كذلك من الأمن القومي والسيادة الوطنية للدول. والأخطر من ذلك كونها تؤدي إلى فقدان الثقة في التعاملات الإلكترونية مما يؤثر على الخطط التنموية الاقتصادية وكذلك مجالات الاستثمار والمشروعات المتعلقة به.

وقد أوضح أحد الخبراء المتخصصين في مكتب الأمم المتحدة لمكافحة الجريمة أن الجرائم الإلكترونية هي جريمة القرون القادمة، ومن ثم يجب توحيد وتضافر الجهود الدولية لمكافحتها. وفي ضوء ذلك سارعت دول مجلس التعاون الخليجي بسن التشريعات الخاصة بمكافحة الجرائم الإلكترونية، ومن أمثلة ذلك ما قامت به دولة الإمارات العربية المتحدة من وضع قوانين لمكافحة جرائم الإنترنت بأنماطها المختلفة حيث أصدرت قانون التجارة الإلكترونية رقم 1 لسنة 2006 م، وقانون مكافحة جرائم تقنية المعلومات رقم 2 لسنة 2006 م أيضاً مع القيام بتعديله بالقانون رقم (5) لسنة 2012 م، وكذلك قامت المملكة العربية السعودية بوضع وثيقة الرياض والتي تضمنت النظام (القانون) الموحد لمكافحة الجرائم الإلكترونية لدول مجلس التعاون لدول الخليج العربية والتي أصدرتها الأمانة العامة لمجلس التعاون لدول الخليج العربية، كما قامت قطر كذلك بإصدار قانون لمكافحة الجرائم الإلكترونية.

وبالرغم من الجهود التي بذلتها كافة دول العالم ومن بينها دول مجلس التعاون الخليجي لغرض الوقاية والمكافحة للجرائم الإلكترونية سواء من خلال سن التشريعات أم وضع الإجراءات الأمنية والتقنية فإن تلك الجرائم ما زالت تشكل خطورة كبيرة على أمن المجتمع الخليجي لا سيما في ظل الاعتماد المتزايد على الأدوات والوسائل الإلكترونية في الغالبية العظمى من مناحي الحياة.

من أجل ذلك سوف يتم في هذا المبحث بيان مفهوم الجرائم الإلكترونية في المطلب الأول وأنماطها في المطلب الثاني ووسائل ارتكابها في المطلب الثالث. وقد وضعت العديد من التعريفات للجريمة الإلكترونية حيث لم يتفق الباحثون والمفكرون على تعريف جامع مانع لها كما تعددت أنماطها في ضوء التنوع في الوسائل الإلكترونية التي يمكن من خلالها ارتكاب تلك الجرائم. وعلى ذلك سوف يتم في هذا المبحث تناول مفهوم الجرائم الإلكترونية في المطلب الأول مع بيان أنماطها في المطلب الثاني على النحو التالي:

المطلب الأول: مفهوم الجرائم الإلكترونية.

المطلب الثاني: أنماط الجرائم الإلكترونية.

المطلب الأول- مفهوم الجرائم الإلكترونية:

وضع العديد من الباحثين والمفكرين من المتخصصين ذوي العلاقة بأدبيات العلوم الجنائية والاجتماعية المختلفة المعنية بدراسة الجريمة تعريفات متعددة للجريمة الإلكترونية.

وفي هذا السياق ذهب البعض إلى تعريف الجريمة الإلكترونية بأنها "تتعلق بالكيانات المعنوية ذات القيمة المادية أو القيمة المعنوية البحتة أو كلاهما معاً، وهذا هو أساسها كما أنها تتكون من عناصر أساسية هي عناصر الجريمة والسلوك والوصف الإجرامي والنص القانوني على تجريم السلوك وإيقاع العقوبة، وهي تهدف إلى الحصول على معلومات الأجهزة والأشخاص والجهات بشكل مباشر، أو تهدف بشكل غير مباشر إلى الأشخاص والجهات المعنية بتلك المعلومات أو الأجهزة عن طريقها". وقد أشار هؤلاء إلى وجود مسميات عدة لتلك الجريمة منها (جرائم عبر الكمبيوتر والإنترنت، جرائم تقنية المعلومات، جرائم أصحاب الياقات البيضاء)[1].

وذهب البعض الآخر إلى أن الجرائم الإلكترونية هي "التي يتم من خلالها استخدام التقنيات الرقمية لإخافة وإخضاع الآخرين، ومن أمثلة ذلك الإرهاب الإلكتروني، وإنّ مصطلح تلك الجرائم يشمل كافة الجرائم المستحدثة والمتعلقة بكل من الحاسبات أو شبكة

1- الدكتور. عماد مجدي عبد الملك، المرجع السابق ص 31.

الإنترنت سواء كانت الحاسبات هي التي يقع عليها فعل الاعتداء أم الجرائم التي تكون فيها الحاسبات أداة في يد الفاعل مرتكب جريمة الاعتداء، وإنّ مصطلح الجريمة الإلكترونية من العمومية بحيث يشمل كافة الأفعال والاستخدامات العديدة التي يصعب حصرها لشبكة الإنترنت العملاقة من الناحية التقنية[1].

كما أوضح باحث ثالث إلى أن الجرائم الإلكترونية تعدّ إحدى أهم صور الجرائم ذات البعد الدولي العابر للحدود وأن تلك الحدود أصبحت لا تشكل حدًّا أو مانعاً لمرتكبي هذه الجرائم، وأن نشاط مرتكبيها وفقاً لذلك لم يعد ممكناً أو واقعاً في النطاق الإقليمي لدولة واحدة، فقط بل يمكن لهم تجاوز هذا النطاق إلى أقاليم أو دول أخرى، كما يمكن لهؤلاء تقسيم النشاط الإجرامي بمراحله المختلفة ليقع كل منها بأحد الأقاليم حتى ولو بعدت بينها المسافات واختلفت التوقيتات، ومن ثم فإنّ تلك الجريمة أصبحت ذات طابع دولي عابر للوطنية وأن مرتكبيها يمكن تصنيفهم تحت نطاق المجرمين الدوليين[2].

وبالإضافة إلى ما سبق، أشار باحث رابع إلى اختلاف الفقه الجنائي في إيجاد مفهوم معيّن للجريمة الإلكترونية أو التقنية نظراً لحداثتها وأنه يمكن تعريفها بأنها "سلوك غير مشروع جنائيًّا موجه نحو إساءة استعمال النظام الآلي لمعالجة المعلومات باستخدام الحاسب الآلي أو أية وسيلة تقنية أخرى[3].

ومن ناحية أخرى، عرّف أحد الباحثين الجريمة الإلكترونية بأنها "كل فعل إيجابي أو سلبي عمدي يهدف إلى الاعتداء على تقنية المعلوماتية أيًّا كان غرض الجاني، وقد أوضح هذا الباحث عدم وجود اتفاق على مصطلح معين للدلالة على تلك الظاهرة المستحدثة،

1- الأستاذ. أمير فرج يوسف، الجرائم المعلوماتية على شبكة الإنترنت، دار المطبوعات الجامعية، الإسكندرية، 2008 م، ص 103-107.

2- الدكتور. عادل عبد العال إبراهيم خراشي، إشكاليات التعاون الدولي في مكافحة الجرائم المعلوماتية وسبل التغلب عليها، دار الجامعة الجديدة، الإسكندرية، 2015 م، الطبعة الأولى، ص 11.

3- الدكتور. نوفل علي عبد الله الصفو، دراسات في القانون الجنائي المقارن (جريمة الإخلال بالآداب العامة بواسطة وسائل تقنية المعلومات)، دار الجامعة الجديدة، الإسكندرية، 2014، 2015 م، ص 127.

فهناك من يطلق عليها ظاهرة الغش المعلوماتي أو الاختلاس المعلوماتي أو الجريمة المعلوماتية، ومن ثم لا يوجد تعريف محدد ومتفق عليه حول تلك الجريمة[1].

وفي ذات السياق بين باحث آخر أن الجرائم الإلكترونية ترتبط بالمجال المعلوماتي وتتصل بالبيانات الالكترونية سواء على المستوى الدولي أم الفردي، وإنّ استخدام الحاسب الآلي أمرٌ ضروريٌّ ولازمٌ لارتكابها، كما يشترط في مرتكبيها أن يصلوا إلى درجة من الاحترافية والكفاءة والخبرة في استخدام الحواسب الآلية، كما أن تلك الجرائم لا تقيد بحدود مكانية أو زمنية معينة مع اختلاف أهداف ارتكاب تلك الجرائم[2].

كما عرفت وزارة الداخلية المصرية الجريمة الإلكترونية بأنها "كل جريمة أو سلوك غير مشروع يستخدم الحاسب الآلي، أو محاولة نسخ أو حذف أو إتلاف برامج الحاسب الآلي، أو أيّ جريمة يكون لتنفيذها صلة بالقواعد أو العلوم المعلوماتية أو أيّ سلوك غير مشروع متعلق بالمعالجة الآلية للبيانات[3].

وممّا سبق يتضح الاختلاف بين الباحثين في تعريف الجريمة الإلكترونية ومن ثم يمكن تعريف تلك الجريمة بأنها " كل فعل أو الامتناع عنه يتم أو كان يجب القيام به باستخدام أدوات التقنيات الإلكترونية وأساليبها الإلكترونية بالمخالفة لما أقره المشرع أو نهى عنه ويستلزم توقيع عقوبة جنائية على من قام بهذا الفعل أو امتنع عن القيام به".

المطلب الثاني - أنماط الجرائم الإلكترونية:

توجد أنماط متعددة للجرائم الإلكترونية، وقد ساهم في هذا الأمر تعدد صور الاستخدام للوسائل التقنية في مجالات الحياة سواء على المستوى الشخصي أم المؤسسي ممّا

1- الدكتور. أشرف عبد القادر قابيل، الإثبات الجنائي في الجريمة الإلكترونية، دار الجامعة الجديدة، الإسكندرية، 2015 م، ص 92-93

2- الأستاذ. نايل نبيل عمر، الحماية الجنائية للمحل الإلكتروني في جرائم المعلوماتية، دار الجامعة الجديدة، الإسكندرية، 2012 م، ص 11.

3- الموقع الإلكتروني لوزارة الداخلية المصرية www.moiegypt.gov.eg

شجع مرتكبي تلك الجرائم على ابتكار أنماط متعدد منها اعتماداً في ذلك على ذكاء المجرم الإلكتروني وتوافر القدرة والمهارة الإلكترونية لديه أو نتيجة لما أفرزنه الثورة التكنولوجية من وسائل عدة أتاحت التفاعل والتواصل بين عدة أطراف في آنٍ واحدٍ من بلدان مختلفة مهما تباعدت بينها المسافات، وعلى ذلك سوف يتم إيضاح صورٍ من أنماط تلك الجرائم وذلك على النحو التالي:

أولاً: السطو الإلكتروني على بيانات بطاقات الائتمان، وقد تعددت الوسائل والأساليب المتبعة من قبل العصابات الإلكترونية في مجال الحصول غير المشروع على بيانات بطاقات الائتمان لغرض استخدامها في عمليات الشراء أو الدفع للحصول على المنافع المختلفة[1].

ومن أمثلة الأساليب الإلكترونية المستخدمة والتي تقوم بها عصابات الإجرام الإلكتروني لغرض الحصول على البيانات والمعلومات الخاصة ببطاقات الائتمان واستخدامها بصورة غير مشروعه الاختراق غير المشروع لشبكة الاتصالات الإلكترونية بين البنوك أو الشركات وعملائهم بغرض الوصول إلى البيانات الخاصة ببطاقات الائتمان وكذلك ما يعرف بتقنية "تفجير الموقع المستهدف" والتي تستخدم لغرض نقل ما به من البيانات والمعلومات الخاصة ببطاقات الائتمان المخزنة إلى الأجهزة الخاصة بالجناة ومن ثم يسهل لهم الحصول عليها واستخدامها، وأيضاً ما يسمى بأسلوب الخداع والذي يعتمد على إقامة مواقع إلكترونية افتراضية على شبكة الإنترنت لاستقبال المعاملات المالية والتجارية الخاصة بالشركات ومن ثم استخدامها بصورة غير مشروعة، وكذلك الصناعة الافتراضية لأرقام البطاقات الائتمانية من خلال استخدام بعض المعادلات الحسابية[2].

1- الأستاذ أمجد حمدان الجهني، جرائم بطاقة الدفع الإلكتروني عبر شبكة الإنترنت، بحث منشور على الموقع الإلكتروني لمركز الدراسات القضائية التحقيق

HTTP://WWW.COISS.COM/REPLOV.PHP.2A،219

2- الدكتور عماد على خليل، التكييف القانوني لإساءة استخدام البطاقات عبر شبكة الإنترنت، مؤتمر القانون والكمبيوتر والإنترنت، جامعة الإمارات العربية، العين، 2000 م، ص 5.

وبالإضافة إلى ما سبق توجد كذلك أساليب أخرى لغرض السطو الإلكتروني على بيانات بطاقات الائتمان من خلال اتباع أساليب للتجسس يقوم بها قراصنة التقنيات للوصول إلى البيانات والمعلومات الخاصة بضحاياهم عبر شبكة الإنترنت والمتصلة ببطاقات الائتمان الخاصة بها لغرض استخدامها في أنشطتهم غير المشروعة[1].

ثانياً: وقد قام أحد الباحثين بوضع تصنيف لأنماط الجرائم الإلكترونية وتوصل في هذا الصدد إلى وجود تصنيفين لتلك الجرائم: الأول حسب مواطن الاختراق وقسمها إلى اختراق الأمن المادي أو اختراق الأمن الشخصي للأفراد أو اختراق الحماية الخاصة بالاتصالات وأمن البيانات، وأخيراً الاعتداء على عمليات الحماية. والثاني هو التصنيف حسب مساس تلك الجرائم بالأشخاص والأموال ومن أمثلتها الجرائم التي تستهدف الأشخاص وتلك التي تستهدف الأموال باستثناء السرقة، أو جرائم الاحتيال والسرقة، أو جرائم التزوير، وكذلك جرائم المقامرة والجرائم الأخرى ضد الأخلاق والآداب وأخيراً جرائم الكمبيوتر ضد الحكومة[2].

ثالثاً: وفي هذا السياق قام باحث بتحديد أنماط الجرائم الإلكترونية بنمطين رئيسيين يتعلق الأول بحالة الاعتداء على المكونات المادية لأجهزة الحاسوب، ومثال ذلك سرقتها أو إتلاف مكوناتها وما يتصل بها من أجهزة تقنية أخرى، وأما النمط الثاني فيتعلق بالاعتداء وعلى المكونات غير المادية والتي تحتويها الحاسبات والأجهزة الإلكترونية، ومثال ذلك السطو أو الحذف أو الإضافة أو الإلغاء أو الإيقاف الدائم أو المؤقت للبيانات والمعلومات المخزنة بالحاسبات أو التي تصل إليها عبر شبكة الاتصالات الدولية الإنترنت أو وسائلها المتعددة[3].

1- الأستاذ. علي حسن عباس، مخاطر بطاقات الدفع الإلكتروني عبر شبكة الإنترنت (المشاكل والحلول)، ورقة عمل قدمت بندوة الصورة المستخدمة لجرائم بطاقات الدفع الإلكتروني، أكاديمية الشرطة المصري، مركز بحوث الشرطة، القاهرة، 1998/2/14 م، ص 25.

2- الأستاذ. أمير فرج يوسف، الجرائم المعلوماتية على شبكة الإنترنت، دار المطبوعات الجامعية، الإسكندرية، 2008 م، ص 50-51.

3- الدكتور. أشرف عبد القادر قنديل، الإثبات الجنائي في الجريمة الإلكترونية، دار الجامعة الجديدة، الإسكندرية، 2015 م،ص 94.

رابعاً: الإخلال بالآداب العامة باستخدام البرامج الإلكترونية، ويشمل هذا النمط الإجرامي كل ما يتعلق بالأفعال الإلكترونية التي يقوم بها الجاني والتي تشكل في حد ذاتها اعتداء على الآداب العامة أو الإخلال بها، ومثال ذلك الإرسال أو الإنتاج أو التخزين أو التهيئة أو الإعداد للصور أو البيانات أو المعلومات التي تمس كيان وأخلاق المجتمع ويعد كذلك من صور الإخلال بالآداب العامة من خلال استخدام الوسائل الإلكترونية أخذ الصور الإباحية للأطفال عن طريق التصوير المباشر لهم تحت تأثير الترهيب أو الترغيب أو عن طريق التلصص والقيام بوضعها عبر الإنترنت[1].

خامساً: جريمة تقليد المصنفات بالحاسب الآلي، ويتمثل السلوك الإجرامي في هذه الجريمة بعملية التقليد للمصنف الإلكتروني أيًا كان نوع هذا الصنف وسواء أكان من المصنفات الفنية أو الأدبية والتي يتم استحداثها على غرار المصنف الأصلي المحمي أم كان عبارة عن مجموعة من البيانات والمعلومات أو الرسوم أو غيره[2].

سادساً: الدخول غير المشروع لأنظمة المعلومات وقواعد البيانات، ويقوم بهذا النشاط الإجرامي من يطلق عليهم المحترفون والذين توجد لديهم المهارة والقدرة التقنية للدخول للمواقع المختلفة بشبكة الإنترنت متفوقين في ذلك على كل وسائل الحماية والأمن الموجودة، ويستهدف المحترفون غالباً الحصول على البيانات أو المعلومات الموجودة على الموقع المخترق أو لإظهار براعتهم في كشف نقاط الضعف في نظم الحماية لتلك المواقع مما يستلزم وضع نظم تأمين أكثر فاعلية لها[3].

1- الدكتور. نوفل علي عبد الله الصفوة، جريمة الإخلال بالآداب العامة بواسطة وسائل تقنية المعلومات، دراسات القانون الجنائي المقارن، دار الجامعة الجديدة، الإسكندرية، ص 133.

2- الدكتور. علي عبد القادر القهوجي، الحماية الجنائية لبرامج الحاسب الآلي، دار الجامعة الجديدة، الإسكندرية، 2011 م، ص16.

3- الدكتور. عماد مجدي عبد الملك، جرائم الكمبيوتر والإنترنت، دار المطبوعات الجامعية، الإسكندرية، 2011 م، ص 64-65.

سابعاً: الاستغلال الجنسي للأطفال عبر شبكة الإنترنت في ضوء ما أتاحته شبكة الإنترنت من التوسع والانفتاح العالمي، قام مستغلو تلك الشبكة على نحو غير مشروع لا سيما فيما يتعلق بالأفعال المتعلقة بالجرائم الجنسية كالتحريض والدعاية للاستغلال الجنسي للأطفال. وقد أشارت إحدى التقارير الدولية في هذا الصدد إلى الاستغلال الجنسي لحوالي 2 مليون طفل معظمهم من الفتيان، وقد ساعد على ذلك ما أفرزته الثورة التكنولوجية والحواسب وشبكة الإنترنت والتي أدت إلى وجود ما يفوق 100 ألف موقع إباحي يتم من خلالها عرض صورٍ للاستغلال الجنسي للأطفال، كما يتم إضافة ما يقارب من 20 ألف صورة للاستغلال الجنسي للأطفال كل أسبوع تقريباً على تلك المواقع وتتراوح أعمار من يتم عرض صورهم من 10 سنين إلى 17 سنة[1].

المبحث الثاني
خصائص وسمات الجرائم الإلكترونية ومخاطرها

بعد أن تم الانتهاء في المبحث الأول من استعراض مفهوم الجرائم الإلكترونية وأنماطها، سوف يتم في هذا المبحث إيضاح خصائص وسمات تلك الجرائم ومخاطرها على النحو التالي:

المطلب الأول- خصائص وسمات الجرائم الإلكترونية:

عدد الباحثون والخبراء الخصائص والسمات التي تتصف بها الجرائم الإلكترونية. وعلى ذلك فإنّ هناك خصائص وسمات عدة لتلك الجرائم من بينها ما يلي:[2]

1- الدكتور. علي كريمي، الشباب وتشريعات الإنترنت العربية، جريمة الاستغلال الجنسي للأطفال نموذجاً. بحث منشور على الموقع الإلكتروني
WWW.MAROC.REUNIS.FR/COMELD/INDEX.PHP

2- الدكتور. أحمد وهدان، تقييم فعاليات المواجهة التشريعية لجرائم الإنترنت، الشارقة، القيادة العامة لشرطة الشارقة، مركز بحوث الشرطة، دورية الفكر الشرطي، المجلد 13، العدد 1، أبريل،2004 م، ص 99.

1. الاختلاف الواضح بين تلك الجرائم وما سبقها من أنماط الجرائم في عصر ما قبل التكنولوجيا. وذلك من حيث أداة الارتكاب والتي كانت تعتمد في الجرائم غير الإلكترونية على الأدوات التقليدية والمعروفة والشائعة الاستخدام والتي تعد في غالبيتها إن لم تكن جميعها من الأدوات ذات المظهر المادي على خلاف الجرائم الإلكترونية والتي يتم ارتكاب غالبيتها من خلال الحيز المعنوي أو غير الظاهر للحواسيب. وكذلك من حيث طبيعة مرتكبي تلك الجرائم إذ إن مرتكبي الجرائم العادية أو القديمة لا يلزم فيهم توافر العلم أو المهارة في اللغة أو في البرمجيات والنظم الإلكترونية، وذلك على خلاف المجرم الإلكتروني الذي يتمتع بالمهارة والحنكة والمعرفة للعديد من العلوم لا سيما في مجال الحواسب وبرامجها بل إنّ هؤلاء يعد العديد منهم من الخبراء والمتخصصين في المجال الإلكتروني.

2. حداثة الجرائم الإلكترونية إذ إنها لم تظهر إلى حيز الوجود إلا منذ أربعة عقود تقريباً متزامنة في ذلك مع شيوع استخدام أجهزة الحاسوب، وذلك على خلاف الجرائم الأخرى والتي عرفها الإنسان منذ بدء الخليقة. المعالجة التشريعية لصور الجرائم التقليدية بكافة دول العالم وذلك في ضوء معرفتها وتحديد أركانها المادية والمعنوية بصورة واضحة وذلك على خلاف الجرائم الإلكترونية التي لم يتناولها المشرع بالتجريم إلا في عدد قليل من الدول لا سيما بالمجتمع العربي وذلك في ضوء حداثة تلك الجرائم وعدم معرفة كافة أنماطها وكذلك عدم الإحاطة الكاملة بأركانها المادية والمعنوية وتوالي الظهور المتسارع لأنماط أخرى جديدة منها في ضوء التطور للتكنولوجيا والتقنيات المستخدمة في ارتكابها. اتساع البعد المكاني والزماني للجريمة الإلكترونية وذلك على خلاف الجرائم الأخرى إذ إن الحيز المكاني لها يمكن أن يمتد ليشمل عدة دول تتم في إحداها الأعمال التحضيرية لارتكابها وفي أخرى أحد الأركان المادية لها أو جزء منها على أن يتم اكتمال ارتكابها في دولة أو دول أخرى. كما يمكن أن يشارك في ارتكابها في آن واحد العديد من الجناة الذين يتواجد كل منهم في قطر مختلف. مما يصعب في كثير من

الأحيان عملية الملاحقة والضبط لهم أو التعرف على مرتكبيها بصورة كاملة في وقت سريع[1].

3. تصنيف الغالبية من الجرائم الإلكترونية بأنها من صنف الجرائم الذكية التي تعتمد في ارتكابها على استخدام المهارات والقدرات والمعارف الذهنية فقط دون الحاجة إلى استخدام العنف وما يلحقه من الضرر البدني بالمجني عليهم. ومن ثـم فـإنّ وجود ظواهر مادية واضحة للعيان في الجرائم الإلكترونية أمر يندر وجوده فيمـا عدا الجرائم التي تقع على الحواسب وملحقاتها بقصد تدميرها أو إتلاف المظهـر المادي لها. صعوبة الوصول إلى شهود في الوقائع المرتبطة بالجرائم الإلكترونية لعدم وجود مظهر مادي خارجي ملموس لها. وذلك بخلاف الجرائم الأخرى التي تقع وتأخذ أشكال مادية مختلفة، ومثال ذلك الإمساك بالمجني عليه أو إطلاق النار عليه أو التعدي عليه بآلة حادة، وكل تلك الأفعال من السهل مشاهدتها في الوسـط المحيط بارتكاب الجريمة في حين أن الجرائم الإلكترونية قد يتم ارتكابها دون أن يلحظ المحيطون بمرتكبها أو الموجودون معه بدائرة تواجده بقيامه بأيٍّ من أفعالها أو أعمالها التحضيرية. اتفاق الجرائم الإلكترونية مع مثيلتها من الجرائم التقليديـة في كثير من الدوافع لارتكابها، ومثال ذلك الحصول على المال بصـورة غيـر مشروعة والإيذاء النفسي والتهديد والإساءة للسمعة والانتقام. قيام الجاني بكلٍّ من الجرائم الإلكترونية والتقليدية بإخفاء أو بإتلاف أو تدمير الأدلة المسـتخدمة فـي ارتكاب الجريمة.

المطلب الثاني- مخاطر الجرائم الإلكترونية:

أظهر الرصد للجرائم الإلكترونية وجود الكثير من المخاطر والمهددات الناجمة عن تلك النوعية من الجرائم والتي تتمثل في الآتي:

1- مقدم الدكتور. سرحان حسن المعيني، التحقيق في جرائم تقنية المعلومات، الشارقة، القياد العامة لشرطة الشارقة، دورية الفكر الشرطي، المجلد 2، العدد 4، 79، أكتوبر 2011 م، ص 27.

1. انتهاك سيادة الدولة وتجاوز حدودها الإقليمية، وتعرف سيادة الدولة بأنها "السلطة العليا للدولة التي لا تعلوها سلطة أخرى والتي لها الحق في تنظيم العلاقات ووضع القوانين، كما تعرف السيادة بأنها: "أن تكون للدولة الكلمة العليا واليد الطولى على إقليمها وعلى ما يوجد فوقه أو فيه في نطاق حدودها الجغرافية المتعارف عليها"، ولا شك أن الجرائم الإلكترونية وبما تصنف به من كونها جرائم عابرة للوطنية قد أدت إلى إلغاء مفهوم السيادة للدولة وما يتصل به من السيطرة والتحكم على ما يأتي إلى أراضيها من الخارج. إذ إن طبيعة تلك الجرائم تسمح بوقوع أفعالها في أكثر من إقليم بدول عدة. كما لا يعوق انتقالها من دولة إلى أخرى أية عوائق في ظل عالمية شبكة الإنترنت وكافة الوسائل والبرامج الإلكترونية الخاصة بأجهزة الحاسوب والتي تمكن مرتكبي تلك الجرائم من القيام بأفعالهم الإجرامية دون اعتبار للحدود الجغرافية الفاصلة. مع عدم استطاعة الدول على التصدي لهذا الأمر أو التعلل بمبدأ السيادة والإقليمية[1].

2. الإقلال من إيجابيات الأدوات والنظم الإلكترونية، لا شك أن الثورة التكنولوجية وما أفرزته من أدوات ووسائل إلكترونية متعددة كان لها الكثير من الإيجابيات، وكذلك البعض من السلبيات. ومن المعروف أن ظهور الجرائم الإلكترونية التي تعتمد في ارتكابها على الأدوات والوسائل التقنية المختلفة وتزايد تلك الجرائم وشمولها لجوانب عدة على المستوى المجتمعي أو الشخصي وعدم اقتصارها في إلحاق الضرر على جهة دون أخرى أدّى إلى تخوف الناس من تلك التقنيات في ظل زيادة سلبياتها ومخاطرها في مقابل ما حققته من إيجابيات وقيام البعض بعدم استخدامها إلا في حالات الضرورة مع الاعتماد على الوسائل التقليدية القديمة التي كانت تتسم بالأمان، وعدم التعرض لمخاطر عدة مقارنة بالجرائم الإلكترونية[2].

1- الأستاذ الدكتور. ربيع أنور فتح الباب، النظم السياسية (السلطة، الدولة، الحكومة صورها وأساليبها)، ج.م.ع، القاهرة، دار نصر للطباعة الحديثة، 2003 م، ص 45.

2- بروفسورة/ دايان مارتن، معالجة مشاكل شبكة ويب العالمية www المسائل الأمنية والاجتماعية المتعلقة بشبكة الإنترنت (أبوظبي)، شرطة أبوظب ، مركز البحوث والدراسات الأمنية ، ورقة عمل قدمت بندوة شباب الإنترنت وتأثيراتها الاجتماعية والأمنية، الطبعة الثانية، 7،6/ نوفمبر 2006 م، ص 301.

3. انتهاك الخصوصية للأشخاص والتعدي على مستودع أسرارهم: تزايد اعتماد الأفراد عقب الثورة التكنولوجية على الأدوات والوسائل الإلكترونية المتعددة والمتنوعة التي أفرزتها تلك الثورة لغرض حفظ بياناتهم ومعلوماتهم الشخصية والتي تتعلق بأمورهم الخاصة الاجتماعية والمالية والتي يرغبون في الاحتفاظ بها وعدم إطلاع الغير عليها حتى أصبحت أجهزة الحاسوب بمثابة مستودع السر الذي يحتفظ بكافة الأسرار والخبايا. ولم يهنأ الأفراد طويلاً في الائتمان على أسرارهم بتلك الأجهزة إذ سرعان ما قام مرتكبو الجرائم الإلكترونية باقتحام المواقع الخاصة بالأفراد والوصول إلى معرفة ما بها من بيانات ومعلومات وقاموا باستغلالها بصورة سيئة سواء على المستوى الاجتماعي أم المالي للأشخاص ممّا أدّى إلى تخوف العديد من الأفراد من الاحتفاظ ببياناتهم ومعلوماتهم الشخصية الهامة بأجهزة الحاسوب. كما قامت الأجهزة الأمنية والإعلامية بالعديد من الدول بتوعية الأفراد بعدم الاحتفاظ ببياناتهم الهامة بتلك الأجهزة في ضوء ما تم اكتشافه من جرائم إلكترونية استهدفت تلك البيانات والمعلومات.

4. نشر الرذيلة والتحريض على الفسق والدعارة وساهم الانتشار العالمي في استخدام الأدوات والوسائل الإلكترونية وهدم الحواجز بين الدول من خلالها على سهولة ويسر نقل العديد من الصور والأفلام التي تتضمن كافة صور الخروج عن الآداب العامة والتي تتضمن الإباحية والخروج عن التقاليد والقيم الاجتماعية الصحيحة. وهو ما كان له أبلغ الأثر الضار والسلبي في المجتمعات العربية لا سيما المجتمعات الخليجية بين الشباب وصغار السن الذين يسهل تأثرهم بتلك الصور والأفلام.

5. التهديد للأمن من خلال زيادة فرص ارتكاب الجرائم: أدى التوسع في الاستخدامات الإلكترونية لأجهزة الحاسوب وشبكة الإنترنت وشبكات التواصل الاجتماعي إلى خلق العديد من الفرص لارتكاب الجرائم، ومن أمثلة ذلك إتاحة نشر المعلومات الخاصة بصنع الأسلحة والمتفجرات والتي يتم استخدامها لغرض

ارتكاب العديد من الجرائم، ومثال ذلك السرقة والسطو والقتل والاعتداء، وكـذلك في الأعمال الإرهابية. وقد أتاحت تلك المواقع ارتكاب جرائم تمثل خطورة كبيرة على أمن المجتمع، ومثال ذلك غسل الأموال والمخدرات والتزييـف والتزويـر والنصب الإلكتروني والسطو الإلكتروني على حسابات البنوك والمؤسسات المالية والأفراد.

6. تهديد البنية الاقتصادية للدول، ويعد هذا الخطر مـن أكثـر مخـاطر الجـرائم الإلكترونية. إذ إنّ مرتكبي تلك الجرائم يعمدون في الغالب عنـد ارتكابهـا إلـى الحصول على أكبر منافع مادية، وقد سهّلت لهم النظم الإلكترونية هـذا المجـال حيث ظهرت إلى حيز الوجود جرائم السطو الإلكتروني على الودائـع والأمـوال الخاصة بالمؤسسات الاقتصادية والمالية الحكومية أو الخاصة بمؤسسات القطـاع الخاص، كما ظهرت أيضا جرائم النصب الإلكتروني التي يتم من خلالها ممارسة عمليات الاحتيال الإلكتروني لغرض قيام المؤسسات الاقتصادية والمالية بتحويـل بعض من أموالها لمواقع إلكترونية وحسابات بنكية خاصـة بمحترفـي الجـرائم الإلكترونية[1].

7. تهديد البنية الإلكترونية للدول والمؤسسات حيث يعمد مرتكبو الجرائم الإلكترونية في الغالب إلى إثبات مهاراتهم وتفوقهم من خـلال قيـامهم بـاختراق الأنظمـة الإلكترونية للدول ومؤسساتها، وكذلك لغرض تعطيل أو إيقاف تلك الأنظمة عـن العمل سواء بشكل مؤقت أم لفترات طويلة أم لغرض الحصول علـى مـا بتلـك الأنظمة من بيانات ومعلومات[2].

1- بروفسور/ بيتر نمرابوسكي، جرائم الحاسب الآلي، الأبعاد العالمية، دولة الإمارات العربية المتحدة، أبوظبي، مركز البحوث والدراسات الأمنية، شرطة أبوظبي، ورقة عمل قدمت بندوة شبكات الإنترنت وتأثيراتها الاجتماعية والأمنية، الطبعة الثانية، 6،7/ نوفمبر 2006 م، ص 319، ص 321.

2- دكتور/ محمـد عبد الحميد، الاتصـال والإعلام على شبكة الإنترنت، القاهرة، عالم الكتب، 2007 م، ص 38.

المبحث الثالث
موقف وسياسة المشرع الإماراتي اتجاه الجرائم الإلكترونية

تعاظمت مخاطر الجريمة في العصر الحديث وتحديداً منذ حدوث الثورة التكنولوجية وما نجم عنها من إفرازات سلبية أدت إلى ظهور نوعٍ جديدٍ غير مألوف من الجرائم ألا وهو "الجرائم الإلكترونية" والتي تعدّ أشد خطراً وأعظم ضرراً من العديد من أنماط الجرائم التقليدية لا سيما في المستوى المهاري والفني لمرتكبيها في مجال استخدام التكنولوجيا أو أدوات ارتكابها أو الحيز المكاني والزماني لها، وكونها تعدّ من الجرائم العابرة للوطنية في الكثير من أنماطها وهو ما يضعف من قدرات وإمكانات وأساليب مواجهتها في حالات عدة.

ومن هذا المنطلق وفي ظل ما شهدته دولة الإمارات العربية المتحدة ولكونها من الدول الرائدة على المستوى العالمي والإقليمي في تعاظم استخدام التقنيات والإلكترونيات في مجالات عدة ووجود العديد من التطبيقات الإلكترونية حتى أصبحت الحياة تعتمد بصفة رئيسية اليوم في كثير من المؤسسات العامة والخاصة وبالغالبية من مناحي الحياة بالدولة على النظم الإلكترونية ممّا أدى إلى تنامي خطر الجرائم الإلكترونية في ضوء الاستخدام المتزايد للوسائل والأدوات الإلكترونية. وفي ضوء ذلك قام المشرع الإماراتي بإصدار التشريعات اللازمة للتعامل ومواجهة الجرائم الإلكترونية ولغرض حماية المجتمع من مخاطرها ومهدداتها[1].

وعلى ذلك سوف يتم في هذا المبحث بيان تلك التشريعات وما تضمنته من الأفعال والسلوكيات التي وضع المشرع عقاباً لها، ويلي ذلك بيان التعديلات التي أجراها المشرع الإماراتي على التشريعات المتعلقة بالجرائم الإلكترونية، وأخيراً بيان اتجاه المشرع

1- مستشار/ محمد أحمد محمد الحمادي، تشريعات مكافحة جرائم تقنية المعلومات في دولة الإمارات وأحكام القضاء، دولة الإمارات العربية المتحدة، أبوظبي، شرطة أبوظبي، مركز الدراسات الأمنية، ورقة عمل قدمت بندوة شبكات الإنترنت وتأثيراتها الاجتماعية والأمنية، الطبعة الثانية، 6،7/ نوفمبر 2006م، ص9.

الإماراتي وسياسته اتجاه الجرائم الإلكترونية بالقانون الجديد الصادر عام 2012 م، وذلـك في المطالب الثلاثة التالية:

المطلب الأول- التشريع الإماراتي الخاص بمواجهة الجرائم الإلكترونية:

سارع المشرع الإماراتي في العام 2006 م بإصدار القانون رقم (2) لسنة 2006 م في شأن مكافحة الجرائم الإلكترونية والذي يعدّ الأول على مستوى الوطن العربي والعديد من الدول الأجنبية لمواجهة الجرائم الإلكترونية، وقد تضمن القانون التعريف بالمعلومات الإلكترونية والبرنامج المعلوماتي ونظام المعلومات الإلكتروني والشبكة المعلوماتية والمستند الإلكتروني للموقع الإلكتروني ووسيلة تقنية المعلومات والبيانات الحكومية.

كما تضمّن القانون في مواده المختلفة تحديداً للأفعال التي تشكل خطـراً وضـرراً للنظم التقنية المستخدمة وأدواتها المختلفة، وكذلك تحديد العقوبات المتعلقة بارتكاب أيٍّ من تلك الأفعال، ومن أمثلة تلك الأفعال:[1]

1. التوصل بغير وجه حق إلى أيّ موقع أو نظام معلوماتي.
2. الإلغاء أو الحذف أو التدمير أو الإنشاء أو الإتلاف أو التغيير أو إعـادة النشـر للبيانات والمعلومات الموجودة بالموقع أو النظام المعلوماتي.
3. التزوير الإلكتروني للمستندات الإلكترونية الحكومية الاتحاديـة أو المحليـة أو الهيئات أو المؤسسات العامة الاتحادية والمحلية.
4. الاستعمال للمستند الإلكتروني المزور مع العلم بتزويره.
5. الإعاقة أو تعطيل الوصول إلى الخدمة أو الأجهزة والبرامج ومصادر البيانـات والمعلومات بأية وسيلة كانت.
6. الإيقاف أو التعطيل أو التدمير أو المسح أو الحذف أو الإتلاف لمحتويات الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات.

1- القانون الاتحادي الإماراتي رقم (2) لسنة 2006 م في شأن مكافحة الجرائم الإلكترونية وتعديلاته بالقانون الصادر عام 2012 م.

7. استخدام الشبكة المعلوماتية لأغراض التهديد والابتزاز للأشخاص أو للاستيلاء على إحدى وسائل تقنية المعلومات.
8. استخدام الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات للوصول بدون وجه حق للبيانات والأرقام الخاصة بالبطاقة الائتمانية.
9. استخدام الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات للإساءة للشعائر الإسلامية أو أحد المقدسات الدينية.

وقد حدّد المشرع العقوبات واجبة التطبيق في حال ارتكاب الأفعال سالفة الذكر وغيرها الواردة بالقانون والتي تمثلت في الحبس والغرامة والسجن المؤقت، وكذلك بعقوبة تبعية تمثلت في الإبعاد للأجنبي. ويلاحظ ممّا سبق أنّ المشرع الإماراتي لم يغفل تجريم الأفعال الماسة بالنظم التقنية والأدوات المستخدمة بها وقام بتحديد تلك الأفعال والنص على العقوبات الخاصة بها.

المطلب الثاني- التعديلات التي أجراها المشرع الإماراتي على التشريعات المتعلقة بالجرائم الإلكترونية:

وبالرغم ممّا سبق لم يتوقف المشرع الإماراتي عند حد إصدار القانون رقم (2) لسنة 2006 م السابق بيانه بل قام بإصدار القانون الاتحادي رقم (5) لسنة 2012 م في شأن مكافحة الجرائم الإلكترونية لغرض مواكبة المتغيرات والمستجدات سواء على الساحة المحلية أم الإقليمية أم الدولية في هذا المجال.

وفي هذا الصدد، قام المشرع الإماراتي بالإضافة والتعديل للقانون الصادر عام 2006 م في العديد من الأمور، والتي تمثلت في الآتي:

1. تضمنت نصوص القانون الجديد ما يتعلق بالأفعال الخاصة بالجرائم الإرهابية والمعاملات والتجارة الإلكترونية وجرائم الإتجار بالبشر وتلك المتعلقة بالسياحة والآثار والأسلحة النارية والذخائر والمتفجرات والأمن الإلكتروني، وهي أمور لم يتم تضمينها بالقانون القديم الصادر عام 2006 م، وكان الهدف من ذلك

مواكبة المتغيرات والمستجدات فيما يتعلق بأنماط الجرائم المستجدة والأنشطة التجارية والمالية المختلفة والأمن المعلوماتي.

2. تضمن القانون الجديد الصادر عام 2012 م في شأن مكافحة جرائم تقنية المعلومات إضافة بعض التعريفات الجديدة التي لم يتضمنها القانون القديم حيث شمل التعريف بـ (المنشآت المالية أو التجارية أو الاقتصادية، إلكتروني، مواد إباحية الأحداث، العنوان البروتوكولي للشبكة المعلوماتية، سري، الالتقاط، الإساءة) وكان الهدف من ذلك شمول القانون للأنشطة والأفعال الإلكترونية غير المشروعة وكذلك لما يتم من عمليات تجارية باستخدام النظم التقنية.
3. اتجاه المشرع الإماراتي إلى تغليظ العقوبات السالبة للحرية وزيادة قيمة الغرامات المالية وكذلك النص على بعض العقوبات التبعية والتكميلية والتدابير وذلك بالقانون الجديد الصادر خلال عام 2012 م خلافاً لما كان عليه الوضع بقانون عام 2006م حيث قام بالنسبة للعقوبات السالبة للحرية بالنص على عقوبة السجن المؤبد في القانون الجديد، وهو الأمر الذي لم يكن موجوداً بالقانون الجديد. وكذلك قيامه بالنص على العقاب على الشروع بنصف عقوبة الجريمة التامة في الجنح بالمادة (40) وهو أيضاً ما لم يتم النص عليه بالقانون القديم.
4. أمّا بالنسبة لعقوبة الغرامة فقد كانت لا تزيد بالقانون القديم عن 200 ألف درهم أمّا بالنسبة للقانون الجديد فقد وصلت قيمتها إلى مبلغ 3 ملايين درهم.
5. وأيضاً نصّ المشرع بالقانون الجديد على اعتبار جرائم تقنية المعلومات ولإيضاح خطورتها على الأمن والمجتمع من الجرائم الماسة بأمن الدولة.
6. وكذلك نصّ المشرع على اعتبار بعض الأفعال أو السلوكيات أو تكرار القيام بها ظرفاً مشدّداً مما يعني تغليظ العقوبة في حق مرتكبيها.
7. كما أضاف المشرع بالقانون الجديد عقوبة تبعية جديدة بخلاف المصادرة والإغلاق الكلي أو الجزئي للمحل أو الموقع، وهي عقوبة الإبعاد للأجنبي في حال ارتكابه إحدى الأفعال التي تم النص عليها بالقانون الجديد.
8. ونص المشرع أيضاً بالقانون الجديد على بعض التدابير الاحترازية بحق مرتكبي إحدى الأفعال التي نص عليها القانون وتمثلت تلك التدابير في (الإشراف، الرقابة، الحرمان، الوضع في مأوى علاجي أو مركز تأهيل).

9. وأخيراً نص المشرع على تخفيف العقوبة أو الإعفاء منها في حال الإبلاغ عنها وذلك لتحفيز مرتكبيها أو من لديه المعلومات بشأنها للإبلاغ عنها لمنع وقوعها أو لكشف مرتكبيها وملاحقتهم والقبض عليهم عقب ارتكابها.

المطلب الثالث- اتجاه وسياسة المشرع الإماراتي تجاه الجرائم الإلكترونية بالقانون الجديد الصادر عام 2012 م:

يمكن إيجاز اتجاه وسياسة المشرع الإماراتي تجاه الجرائم الإلكترونية بالقانون الجديد الصادر عام 2012 م في ضوء ما سبق في الآتي:

1. تجريم الأفعال الخاصة بالجرائم الإرهابية والمعاملات والتجارة الإلكترونية وجرائم الإتجار بالبشر، وتلك المتعلقة بالسياحة والآثار والأسلحة النارية والذخائر والمتفجرات وما يتعلق بالأمن الإلكتروني.
2. إضافة بعض التعاريف الجديدة وهي: (المنشآت المالية والتجارية والاقتصادية، إلكتروني، مواد إباحية الأحداث، العنوان البروتوكولي للشبكة المعلوماتية، سري، الالتقاط، الإساءة).
3. النص على عقوبة السجن المؤبد.
4. النص على العقاب على الشروع بنصف عقوبة الجريمة التامة في الجنح.
5. زيادة قيمة عقوبة الغرامة المالية إلى مبلغ 3 ملايين درهم بالنسبة لبعض الأفعال والسلوكيات المجرمة بنصوص القانون.
6. اعتبار البعض من الأفعال أو السلوكيات المتعلقة بالجرائم الإلكترونية من الجرائم الماسة بأمن الدولة.
7. اعتبار أيّ جريمة منصوص عليها بالقانون جريمة ماسة بأمن الدولة إذا ارتكبت لحساب أو مصلحة دولة أجنبية أو جماعة إرهابية أو مجموعة أو جمعية أو منظمة أو هيئة غير مشروعة.
8. النص على اعتبار بعض الأفعال أو السلوكيات التقنية من الظروف المشددة التي تستوجب تغليظ العقوبة.
9. النص على عقوبة تبعية جديدة وهي عقوبة الإبعاد للأجنبي في حال ارتكابه إحدى الأفعال أو السلوكيات المجرمة التي نص عليها القانون الجديد وذلك خلاف المصادرة والإغلاق الكلي أو الجزئي للمحل أو الموقع.

10. النص على بعض التدابير الاحترازية بحـق مرتكبـي الأفعـال والسـلوكيات المجرمة بالقانون وهي: (الإشراف، الرقابة، الحرمان، الوضـع فـي مـأوى علاجي أو مركز تأهيل)، وذلك بخلاف العقوبات الأصلية للجريمة والعقوبـات التبعية أو التكميلية لها
11. تخفيف العقوبة أو الإعفاء منها في حال الإبـلاغ عـن أيٍّ مـن الأفعـال أو السلوكيات المنصوص عليها قبل الكشف عنهـا أو للكشـف عـن مرتكبيهـا والمساهمة في التوصل إليهم أو القبض عليهم.

ممّا سبق يتضح أنّ المشرع الإماراتي كان حريصاً منذ البداية وعقب ظهور الجرائم الإلكترونية والتيقن من مخاطرها وأضرارها على الأمن والمجتمع على تجريمها، بـل لـم يكتفِ بذلك وقام بمواكبة كافة المتغيرات والمستجدات ذات الصلة بهذا الأمر فسارع إلـى تعديل نصوص القانون الصادر عام 2006 م في شأن مكافحة جـرائم تقنيـة المعلومـات بالقانون الصادر خلال العام 2012 م. وهو الأمر الذي يدل على حرص دولـة الإمـارات على تحقيق الأمن والأمان بصفة مستمرة ورصد كافة الظواهر الإجرامية والعمـل علـى الوقاية منها ومكافحتها على كافة الأصعدة المحلية والإقليمية والدولية.

الخاتمة

من المعروف أن ّالجريمة الإلكترونية تعني أيّ جريمة يتم ارتكابها باسـتخدام الأدوات والوسائل التقنية، ومثال ذلك شبكة الإنترنت وأجهزة الحاسب الآلي، فهي تعدّ مخالفة ترتكـب ضد أحد الأفراد أو الدولة أو إحدى مؤسساتها أو إحدى المؤسسات الخاصة للعديد من العوامل والأسباب منها على سبيل المثال لا الحصر: التهديد أو الإساءة للسمعة أو الإتلاف والتدمير أو لغرض التجسس أو السرقة، سواءً أكان ذلك بطريقة مباشرة أم غير مباشرة.

وقد شهد التاريخ ارتكاب الجرائم الإلكترونية منذ فترة قاربت الخمسين عاماً، وقـد مر ارتكاب تلك الجرائم خلال تلك الفترة بمراحل عدة بدأت الأولى منهـا عقـب شـيوع

استخدام الحاسب الآلي في الستينات حتى العام 1970 م، وقد انحصرت تلك الجريمة خلال تلك المرحلة في التلاعب بالبيانات المخزنة وتدميرها. ثم بدأت المرحلة الثانية في الثمانينات مع ظهور مفهوم جديد لجرائم الكمبيوتر والإنترنت تمثل في اقتحام الأنظمة ونشر الفيروسات، وتلى ذلك ظهور المرحلة الثالثة في التسعينيات حيث شهدت هذه المرحلة تناميًا هائلاً في حقل الجرائم الإلكترونية، نظرا لانتشار الإنترنت في هذه الفترة ممّا سهل من عمليات دخول الأنظمة واقتحام شبكة المعلومات ومثال ذلك تعطيل الأنظمة الإلكترونية ونشر الفيروسات.

ولا شك أنّ شبكة الإنترنت تعتبر أكبر شبكة للتواصل في العصر الحديث حيث أتاحت الفرصة للتفاعل والتواصل بين الغالبية العظمى من سكان العالم، كما هيّأت المجال لظهور نوعيات مستجدة من الجرائم لم يألفها العالم من قبل.

وقد تعدّدت مخاطر وأضرار تلك الجريمة الإلكترونية التي تمثل أخطر أنواع الصراع بين التقدم التكنولوجي والحفاظ على أمن المجتمعات والمؤسسات والأفراد، ويوماً بعد يوم يشهد العالم خسائر وأضرار عديدة للجرائم الإلكترونية حيث يقال إن عدد السرقات السنوية من قبل مرتكبي تلك الجرائم قد تجاوز أكثر من مليوني حالة، إضافةً إلى مئات الآلاف من الشركات التي وقعت ضحية من قبل القراصنة والمتلصصين، وذلك بسبب نقص أو عدم فاعلية التشريعات الموضوعة، وكذلك الخلل وعدم الإحكام في وسائل الأمن لحماية المواقع الإلكترونية وهو الأمر الذي ينبئ أن تتضاعف أعداد الجرائم الإلكترونية المرتكبة.

ولكل ذلك بات من الضروري أن تواكب التشريعات المختلفة هذا التطور الملحوظ في الجرائم الإلكترونية؛ فالمواجهة التشريعية ضرورية للتعامل من خلال قواعد قانونية غير تقليدية لهذا الإجرام غير التقليدي. مواجهة تتعامل بشكل عصري متقدم مع تلك النوعية من الجرائم التي يأتي في مقدمتها بناء ونشر برامج فيروسات الحاسب الآلي والدخول غير المشروع على شبكات الحاسبات، والتحايل على نظم المعالجة الآلية للبيانات وإتلاف البرامج وتزوير المستندات المعالجة إلكترونيًّا، فضلا عن الجرائم التي تحدث في مجال البنوك.

من أجل ذلك سارع المشرع الإماراتي في العام 2006 م بإصدار القانون رقم (2) لسنة 2006 م في شأن مكافحة جرائم تقنية المعلومات الذي يعدّ الأول على مستوى الوطن العربي والعديد من الدول الأجنبية لمواجهة الجرائم الإلكترونية وقد تضمن القانون التعريف بالمعلومات الإلكترونية والبرنامج المعلوماتي ونظام المعلومات الإلكتروني والشبكة المعلوماتية والمستند الإلكتروني للموقع الإلكتروني ووسيلة تقنية المعلومات والبيانات الحكومية.

وبالرغم مما سبق لم يتوقف المشرع الإماراتي عند حد إصدار القانون رقم (2) لسنة 2006 م بل قام بإصدار القانون الاتحادي رقم (5) لسنة 2012 م في شأن مكافحة جرائم تقنية المعلومات لغرض مواكبة المتغيرات والمستجدات سواء على الساحة المحلية أم الإقليمية أم الدولية في هذا المجال.

وعلى ذلك تناولت هذه الدراسة بيان سياسة المشرع الإماراتي لمواجهة الجرائم الإلكترونية، من خلال البيان لماهية الجرائم الإلكترونية وأنماطها وخصائصها وسماتها ومخاطرها، وكذلك التعريف بالتشريعات الموجودة بدولة الإمارات للتعامل مع تلك النوعية من الجرائم، وأخيراً بيان موقف المشرع الإماراتي وسياسته في التعامل مع تلك النوعية من الجرائم.

النتائج

خلصت هذه الدراسة إلى مجموعة من النتائج تتمثل في الآتي:

1. إنّ هناك مخاطر وأضرار عديدة تشكلها الجرائم الإلكترونية بأنواعها المختلفة.
2. عدم اقتصار المخاطر والأضرار التي تشكلها الجرائم الإلكترونية على جانب أو مجال واحد إذ تتسم تلك المخاطر والأضرار بالتعدد والتنوع.
3. إنّ هناك جوانب قانونية جديدة يجب على المشرع القانوني مراعاتها عند إعداد وصياغة القوانين المنظمة للتعامل مع الجرائم الإلكترونية بأنواعها المختلفة.

4. وجود الكثير من الإشكاليات القانونية المتعلقة بالجرائم الإلكترونية لاختلاف طبيعتها عن الجرائم التقليدية ممّا يستلزم من المشرع التعرف الدقيق على تلك الإشكاليات حتى يتسنى معالجتها على النحو الصحيح.
5. ليس من المتصور وجود سياسة تشريعية واحدة لدى كافة الدول للتعامل مع الجرائم الإلكترونية، فيمكن أن تكون لكل دولة سياسة تشريعية تتبعها، وبالتالي ليس من الضروري أن تتطابق سياستان تشريعيتان لدولتين أو أكثر تطابقاً تامًّا في ضوء المتغيرات الاجتماعية والاقتصادية والأمنية والسياسية لكل منها.
6. إنّ المشرع الإماراتي كان مواكباً للتغيرات التكنولوجية والمعلوماتية والاقتصادية والاجتماعية التي أدت إلى ظهور الجرائم الإلكترونية على المستوى العالمي وشيوعها في العديد من دول العالم والتنبئ بأضرارها ومخاطرها.
7. اهتمام المشرع الإماراتي باتباع سياسة تشريعية جنائية هدفت إلى بيان كافة لأفعال والسلوكيات التي تعدّ من قبيل الجرائم الإلكترونية مع وضع العقوبات اللازمة حيالها.
8. عدم اقتصار المشرع الإماراتي على العقوبات الأصلية لمواجهة الجرائم الإلكترونية بل تعدّى ذلك إلى النص على عقوبات تبعية وتكميلية في حال ارتكاب بعض أنماطها.

التوصيات

انتهت هذه الدراسة إلى مجموعة من التوصيات تتمثل في الآتي:

1. ضرورة التعاون والتنسيق الدولي مع المنظمات ومؤسسات التشريع للتعرف على السياسات التشريعية المختلفة المتبعة بالعديد من دول العالم ومدى الاستفادة منها في تفعيل السياسات التشريعية المعمول بها من قبل المشرع الإماراتي.
2. المراجعة المستمرة والدورية من قبل المشرع الإماراتي للسياسة التشريعية الموضوعة للتعامل مع الجرائم الإلكترونية مع العمل على تعديلها في حال بيان عدم فعاليتها أو ظهور أية متغيرات أو مستجدات تتطلب تعديلها.

3. الحرص في السياسات التشريعية المتبعة على مراعاة مدى التناسب أو التـوازن بين جسامة الضرر أو الخطر ومقدار العقوبة.
4. مراعاة عدم اقتصار فلسفة السياسة التشريعية المتبعة على فكرة ارتباط العقوبـة بجسامة الفعل بل يجب الوضع في الاعتبار شخص الفاعـل وظروفـه النفسـية والاجتماعية والاقتصادية.

المراجع

1. الدكتور. أحمد وهدان، تقييم فعاليات المواجهة التشريعية لجرائم الإنترنت، الشارقة، القيادة العامة لشرطة الشارقة، مركز بحوث الشرطة، دورية الفكر الشرطي، المجلد 13- العـدد 1-أبريـل- 2004 م.
2. الدكتور. أشرف عبد القادر قابيل، الإثبات الجنائي في الجريمة الإلكترونية، دار الجامعة الجديدة، الإسكندرية، 2015 م.
3. الأستاذ . أمير فرج يوسف، الجرائم المعلوماتية على شبكة الإنترنت، دار المطبوعات الجامعيـة، الإسكندرية، 2008 م.
4. البروفسور. بيتر نمرابوسكي، جرائم الحاسب الآلي، الأبعاد العالمية، دولـة الإمـارات العربيـة المتحدة، أبوظبي، مركز البحوث والدراسات الأمنية، شرطة أبوظبي، ورقة عمل قـدمت بنـدوة شبكات الإنترنت وتأثيراتها الاجتماعية والأمنية، الطبعة الثانية، 6-7/ نوفمبر 2006م، ص 319.
5. البروفسوره. دايان مارتن، معالجة، مشاكل شبكة ويب العالمية www المسائل الأمنية والاجتماعية المتعلقة بشبكة الإنترنت (أبوظبي)، شرطة أبوظبي، مركز البحوث والدراسات الأمنية، ورقة عمل قدمت بندوة شباب الإنترنت وتأثيراتها الاجتماعية والأمنية، الطبعة الثانية، 6-7/ نـوفمبر 2006 م.
6. الدكتور. عماد مجدي عبد الملك، جرائم الكمبيـوتر والإنترنـت، دار المطبوعـات الجامعيـة، الإسكندرية، 2011 م.
7. الدكتور. عادل عبد العال إبراهيم خراشي، إشكاليات التعـاون الـدولي فـي مكافحـة الجـرائم المعلوماتية وسبل التغلب عليها، دار الجامعة الجديدة، الإسكندرية، 2015 م، الطبعة الأولى.
8. الدكتور. نوفل علي عبد الله الصفو، دراسات في القانون الجنائي المقارن (جريمة الإخلال بالآداب العامة بواسطة وسائل تقنية المعلومات)، دار الجامعة الجديدة، الإسكندرية.

9. ناير نبيل عمر، الحماية الجنائية للمحل الإلكتروني في جرائم المعلوماتي ، دار الجامعة الجديدة، الإسكندرية، بدون طبعة، 2012 م.
10. الدكتور. عماد علي خليل، التكييف القانوني لإساءة استخدام البطاقات عبر شبكة الإنترنت، مؤتمر القانون والكمبيوتر والإنترنت، جامعة الإمارات العربية، العين، 2000 م.
11. الأستاذ. علي حسن عباس، مخاطر بطاقات الدفع الإلكتروني عبر شبكة الإنترنت (المشاكل والحلول)، ورقة عمل قدمت بندوة الصورة المستخدمة لجرائم بطاقات الدفع الإلكتروني، أكاديمية الشرطة المصرية، مركز بحوث الشرطة، القاهرة، 1998/2/14 م.
12. الدكتور. علي عبد القادر القهوجي، الحماية الجنائية لبرامج الحاسب الآلي، دار الجامعة الجديدة، الإسكندرية، 2011 م.
13. المقدم الدكتور. سرحان حسن المعيني، التحقيق في جرائم تقنية المعلومات، الشارقة، القياد العامة لشرطة الشارقة، دورية الفكر الشرطي، المجلد 2، العدد 4، 79- أكتوبر 2011م.
14. الأستاذ الدكتور. ربيع أنور فتح الباب، النظم السياسية (السلطة، الدولة، الحكومة صورها وأساليبها)، ج.م.ع، القاهرة، دار نصر للطباعة الحديثة، 2003 م.
15. الدكتور. محمد عبد الحميد، الاتصال والإعلام على شبكة الإنترنت، القاهرة، عالم الكتب، بدون طبعة، 2007 م.
16. المستشار. محمد أحمد محمد الحمادي، تشريعات مكافحة جرائم تقنية المعلومات في دولة الإمارات وأحكام القضاء، دولة الإمارات العربية المتحدة، أبوظبي، شرطة أبوظبي، مركز الدراسات الأمنية، ورقة عمل قدمت بندوة شبكات الإنترنت وتأثيراتها الاجتماعية والأمنية، الطبعة الثانية، 6-7/ نوفمبر 2006 م.
17. القانون الاتحادي الإماراتي رقم (2) لسنة 2006 م في شأن مكافحة الجرائم الإلكترونية وتعديلاته بالقانون الصادر عام 2012 م.
18. الموقع الإلكتروني لوزارة الداخلية المصرية www.moiegypt.gov.eg
19. أمجد حمدان الجهني، جرائم بطاقة الدفع الإلكتروني عبر شبكة الإنترنت، بحث منشور على الموقع الإلكتروني لمركز الدراسات القضائية التحقيق HTTP://WWW.COISS.COM/REPLOV.PHP.2A-219
20. الدكتور. علي كريمي، الشباب وتشريعات الإنترنت العربية، جريمة الاستغلال الجنسي للأطفال نموذجاً. بحث منشور على الموقع الإلكتروني WWW.MAROC.REUNIS.FR/COMELD/INDEX.PHP